UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/617,913	07/17/2000	Richard W. Reece	11382.100A	8353

7590 04/20/2004

PATTON BOGGS LLP
2550 M Street, N.W.
Washington, DC 20037

EXAMINER	
SEAL, JAMES	

ART UNIT	PAPER NUMBER
2135	12

DATE MAILED: 04/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/617,913	REECE, RICHARD W.	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 05 December 2004

2. Claims 1-5 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 and 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunstadt US 5003598 A, and further in view of Rabin, Transaction Protection by Beacons 1983.

4. As per claim 1, the limitation of an encryption station and a decryption section for encrypting plaintext into ciphertext is taught by Kunstadt (see Column 1, lines 35-40, Column 2, lines 37-38). The limitation of extracting keying material use for encryption and decryption of messages from a unrelated publicly available broadcast station being readily and reliably available at both sending (encryption station) and receiving (decryption station) locations is taught (Abstract, Column 1, lines 43-45, Column 2, lines 5-8). The limitation of selecting a portion of the public available broadcast station based upon *predetermined secret information* (applicant's private key) is disclosed by Kunstadt in the Abstract. Kunstadt is silent on using the unrelated publicly available broadcast station to transmit random number (Kunstadt method teaches the use of an

unrelated publicly available broadcast station to provide key material for an encryption and decryption station.)

5. Michael O. Rabin (Transaction Protection by Beacons) discloses the use of a beacon transmitting a sequence of randomly generated integers equally spaced in time from a satellite or a node in a network in which is equally accessible all participants, for the purpose of digitally signing contracts using a public key system when the two parties are remotely separated (Abstract and fifth paragraph page 237, and paragraph 1-4 page 258). One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teaching of Kunstadt and Rabin because creating keying materials from random numbers guarantees that the key will be random and hence the encryption most secure. Claim 1 is rejected.

6. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunstadt and Rabin as applied to claim 1 above, and further in view of Maurer US 5161244 A.

7. As per claim 2, the limitation of generating a synchronization signal (generating a time reference signal see Column 1, line 67, Column 2, lines 16-19) is disclosed by Kunstadt using, for example, WWV (time station, see Column 1, line 52-53). The limitation of selecting a portion of the public available broadcast station based upon *predetermined secret information* (applicant's private key) is disclosed by Kunstadt in the Abstract. As per the limitation of generating a sample block of bits based on time t see Rabin page 258-259 section 3, (The Beacon) and in particular 260 comment 1. the

limitation of accumulation random bits and storing them in memory (random number bit reservoir) is not taught by either Kunstadt or Rabin.

8. Maurer teaches the storage of random string strings in memory for later use at both sites (see figure 1, Column 8, lines 19-20, Column 12 lines 50-52). One of ordinary skill in the art would have been motivated to modify the Kunstadt/Rabin teaching without storage with Maurer's teaching of a with storage (random number reservoir) because it would alleviate the demand on the Kunstadt/Rabin system during peak usage and would provide extra security because the random number strings are now delayed (that is, it decreases the likelihood that an attacker simply recording the bits and correlates them against messages as the required storage needed by the attacker would then increase). Further such a modification encryption is perfect as long as the key (consisting of random bits) is as long as the message to be encrypted. Thus for long messages one would have to provide storage to accumulate necessary bits for encryption. Claim 2 is rejected.

9. As per claim 3, the limitation of determining the number of random bits that have been accumulated in memory, and comparing this number with a predetermined full value and if the number is less than the *predetermined* (full value) accumulate and store more bits. Consider figure 1 in Maurer. It is apparent from the figure that the random number generator RAN may be used either to directly encrypt the message the message or to accumulate random bits for the storage means STA (see doted line). The examiner asserts that storage devices must have finite capacity and thus must contain some feedback mechanism to which compares the amount of memory used to

the value when filled or some predetermined value, and to stop the accumulation process at that point. Failure to do so, would result is a waste of computer resources, both memory and computational. Claim 3 is rejected.

As per claim 4, the limitation of generating a new private key (new *predetermined secret information*) is disclosed by the Kunstadt/Rabin/Maurer combination. Maurer discloses the use of threshold storage (see Figure 1) as one means for global encryption (as opposed to direct encrypting). Maurer's RAN in the Kunstadt/Rabin/Maurer combination, would be replaced by Rabin's random number beacon using Kunstadt's predetermined secret information to refill the storage reservoir when the indicator went below some predetermine value. Again one of ordinary skill in the art would have been motivated to modify the Kunstadt/Rabin teaching without storage with Maurer's teaching of a refillable random number reservoir because it would alleviate the demand on the Kunstadt/Rabin system during peak usage and would provide extra security because the random number strings are now delayed. Claim 4 is rejected.

10. As per claim 5, the limitation that the station used for dispersing random number (beacon) be a satellite is disclosed by Rabin (page 257, paragraph 4). Claim 5 is rejected.

11. As per claim 6 (new), the limitation of encrypting data is disclosed by Kunstadt (Column 1, lines 35-45). Kunstadt uses keying material extracted from an publicly broadcasted unrelated signal (see abstract, Figure 1, elements 41, indicates the extraction process and the radio antenna indicates reception of a public broadcast. Further Kunstadt indicates the use of his invention for mobile cellular telephones which

would also necessitate a publicly broadcasted signal, See Column 1, lines 12-14). Kunstadt is silent on the nature of the keying material, however, one of ordinary skill in the art at the time the invention was made would have been motivated to use Rabin random number beacon, because random number are the most secure keying material. Kunstad also discloses a synchronizing means (Column 1, line 42 and 52-53). The extracted feature from the unrelated signal is then used to generate a private key which would indicate the interval (e.g., with regards to the timing station plus other information see figure 1, 21, 41, 13, Abstract, Column 1, lines 35-45). Kunstad's transmitting station is in synchronization with the receiving station then can *select* a piece (interval) of the extracted material of the unrelated signal as a private key which is then used to encrypt (see Figure 1, element 13) and decrypt (element 51) the input message (element 11). As the extracted information from Rabin's beacon (Kunstad's unrelated signal) is a stream of random numbers, the interval chosen by the transmitter and receiver to encrypt the message will be a subinterval of that stream. Providing a message symbol sequence to the encryption device is disclosed Kunsadt Figure 1 11 and 13. As is well known in the cryptographic art a message consists of message symbols (alphabets) with which the encryption device applies substitution or transposition or combination thereof. The encryption device outputs an encrypted message which is then transmitted (see figure 1, elements 13, 14, and 22). Claim 6 is rejected.

12. As per claim 7 (new), the limitation of transmitting encrypted symbol sequence (encrypted message) from the encryption station to the decryption station is disclosed figure 1, elements 13, 14, 22, 14, and 51. The limitation of selecting at the decryption

station a subsequence of random numbers (see explanation in claim 6) that is a portion of the extract of the unrelated signal as determine by the private key is disclosed by the combination of Kunstadt/Rabin. The limitation of decrypting the encrypted symbols sequence at the decryption station based on said decrypting subsequence, to output a message sequence is disclosed by Kunstadt Figure 1, elements 51, 12, and 52. Claim 7 is rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

13. Applicant's arguments filed 05 December 2004 have been fully considered but they are not persuasive. With regards to the comments in reference to claim 1: Applicant states Kunstadt lacks the transmission of random numbers. In response, the examiner notes that Kunstadt was not used for transmission of random numbers.

Kunstadt was used because he recites using unrelated signal as keying data to encrypt and decrypt data and the use of time stations such as WWV to synchronize the use of such keying material at both the transmitter and receiving sites. Rabin was used for the disclosure of transmission of random numbers (as a radio beacon) to both the transmitter and receiver sites. Rabin discloses the use of these random number streams for use in cryptographic protocols (digitally signing documents). Now Kunstadt does not disclose the nature of the keying material as noted above, but one of ordinary skill in the art would have been motivated to combine the unspecified and unrelated keying material received at the transmitter site of Kunstadt with the random numbers being sent out by Rabin because *unless* keying material is *random* and message encrypted with that key can easily be cryptanalysized as send again and again (See David Kahn The Codebreakers for examples of breaking a cipher which used non random or almost random data). Applicant further asserts that a modification would destroy Kunstadt's principle of operation and render it useless for its intended purpose but does not explain as to why it would render Kunstadt system useless. Examiner notes that Kunstadt's invention addresses the encryption of data using keying material from an *unrelated* signal (Abstract). As noted above for keying material to be secure, it must be random and this is precisely what Rabin has to offer and this would not render Kunstadt system useless but in fact make it more secure. Applicant further asserts that Kunstadt or Rabin does not teach or suggest selecting, at the transmitter, a subsequence of the publicly broadcast sequence based on a private key, and encrypting data based on the selected subsequence and further decrypting at the

receiver site the transmitted signal based on the private information. The examiner disagrees. Kunstadt along teaches transmission of data using an unrelated signal as keying material (Abstract, and column 1, lines 35-45). Further he discloses that this unrelated signal used as keying material is publicly broadcast (see Figure 1, element 41 which receives the unrelated signal from a radio antenna element 21 and thus a publicly broadcasted source). Further he discloses that there is a means of synchronizing events between the transmitter and receiving sites (e.g. WWV which transmits time signal Column 1, line 52-53). The time signal enables Kunstadt's transmitting site to tag and label and select the portions of the unrelated signal to be used as keying material in the encryption of the plaintext signal. The keying material (that is the unrelated signal) thus is used to encrypt the message to be transmitted and the interval of unrelated signal which was selected by the transmitter site must remain secret (or private) and known only be the transmitting and receiving site or a third part could easily intercept the encrypted signal and the publicly broadcast unrelated signal and break the encryption. Again Kunstadt is silent on the form of the keying material other than it is derived from publicly broadcast unrelated signal (see abstract, Figure 1, elements 41 for extraction of feature). Was regards to Maurer, Maurer was brought in only to teach storage of random number, that is delayed use of keying material. With regards to the sampling time t based on the input private key (is disclosed in Kunstadt, see above). If Kunstadt must transmit a message of a given length and must use the keying material extracted from the unrelated signal to encrypt the information, then he must extract the appropriate number of bits from the unrelated signal (in this case

Rabin's Beacon) to accommodate the signal. Thus the extraction process must take into account the number of bits to encrypt the message and this with the interval of unrelated signal to exact the bits determines the sampling rates. Again only the transmitter and receiving sites know the interval to be used (that is where the keying material is to be extracted, that is, the private key).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-872-9306. The fax phone numbers for the organization where this application or proceeding is assigned are 703 746 7239 for regular communications and 703 746 7240 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

JWS

Jws
AU 2135
April 18, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100